Notice of Allowability	Application No.	Applicant(s)	
	09/365,211	ULLY, KLAUS	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9/1/04*.

2. ☒ The allowed claim(s) is/are *1-14*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date 02122005.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Examiner's Statement

1. The Applicant is required to submit formal drawings. Drawings are to be submitted to Draftsperson.

Reasons for Allowance

2. Claims 1-14 are allowable for the features of, "includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed.

3. In the prior art of networking, prior art fails to suggest or disclose, includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed. An example of prior art that fails to disclose or suggest, the limitations above, is Sprunk. Sprunk discloses clocking the cryptographic processor to reduce its vulnerability to attack. The clock that is used in Sprunk is ring oscillator that uses a variable delay element. Thus, the clock pulses of Sprunk are unpredictable, because they are random. Thus, the prior art of Sprunk is in contrast, to the claimed limitations of to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm

includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed.

4. In the prior art of security, prior art fails to suggest or disclose, includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed. An example of prior art that fails to disclose these limitations is Silverbrook. Silverbrook discloses an authentication chip that includes a detection unit to prevent power supply attacks. The detection unit of Silverbrook is able to detect, various kinds of attacks including plaintext attacks, and quantum computer attacks. In contrast, to the claimed invention, Silverbrook fails to disclose includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed.

5. In the prior art of non-patent literature, prior art fails to suggest or disclose, includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed. An example of non-patent literature that fails to disclose

the limitations above, is Van. Van teaches a digital signal processor that has an analog signal or continuously varying signals are converted to digital form. It fails to suggest or disclose sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm includes a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

February 12, 2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100